Amendments to the Specification:

Please replace the paragraph at page 41, lines 7-16 with the following rewritten paragraph:

The challenge generation unit 20 randomly generates challenge c, which is query information for authentication. The response verification unit 21 uses the public key y obtained from the certificate verification unit 18, the commitment w obtained from the commitment output unit 11 of the proving instrument before generating the challenge c, and the challenge c generated by the challenge generation unit ~~22~~ 20 to verify the response r obtained from the response output unit 11 of the proving instrument.

Please replace the paragraph at page 42, lines 9-17 with the following rewritten paragraph:

In this embodiment, referring to FIG. ~~10~~ 12, a description will be made of a device that, when a unique value d and a message M are inputted, issues a certificate C used in the certificate type authentication device (the seventh or ninth embodiment) using the proving instrument (the second or sixth embodiment) issued in association with the unique value d by using the hash value generator (the first embodiment). FIG. ~~10~~ 12 is a block diagram of the certificate issuing device.